

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Motorola Model XT1924-7 mobile phone with IMEI
354138095267589; and Black nylon Eastsport backpack

Case No. 19-m-102 (DEJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B.

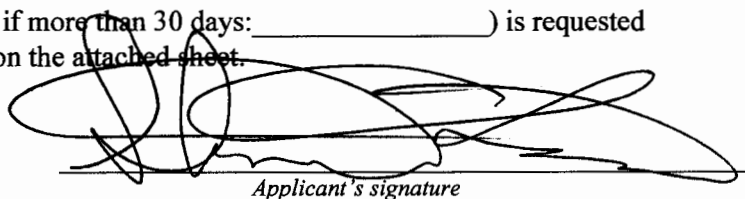
The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of:
violated 18 U.S.C. § 922(g)

The application is based on these facts: See attached affidavit.

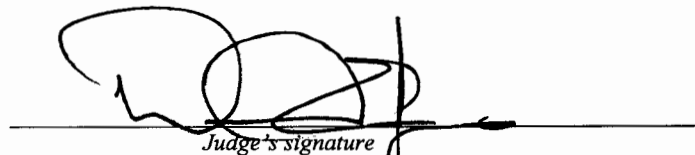
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Shawn M. Friedbacher, Task Force Officer
Printed Name and Title

Sworn to before me and signed in my presence:

Date: April 30, 2019


Judge's signature

City and State: Milwaukee, Wisconsin

David E. Jones, U.S. Magistrate Judge

AFFIDAVIT IN SUPPORT CRIMINAL COMPLAINT AND SEARCH WARRANT

I, Shawn M. Friedbacher, being first duly sworn on oath, depose and state as follows:

I. BACKGROUND, TRAINING & EXPERIENCE

1. I am a Detective with the Waukesha County Sheriff's Department currently assigned as a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI), Milwaukee Field Office. I have been employed as a law enforcement officer in the State of Wisconsin for 24 years.

2. I have gained experience conducting investigations through formal training and consultation with local, state, and federal law enforcement agencies as well as from law enforcement investigations themselves. I have assisted in multiple criminal investigations and participated in numerous search and arrest warrants related to such investigations.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses that I have found to be credible and reliable. This affidavit is intended to show merely that there is sufficient probable cause to support a criminal complaint and corresponding arrest warrant and a search warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe evidence of a violation of 18 U.S.C. § 922(g) will be found on CROCKETT's mobile phone, more particularly described as a Motorola Model XT1924-7, IMEI 354138095267589 (and at Attachment A) ("SUBJECT PHONE").

5. Based on my training and experience and the facts set forth in this affidavit, there is also probable cause to believe evidence of a violation of 18 U.S.C. § 922(g) will be found in the a black nylon Eastsport backpack CROCKETT possessed on April 26, 2019, more particularly described at Attachment A.

II. PROBABLE CAUSE

6. CROCKETT is the subject of an FBI investigation and was previously convicted in the State of Virginia of multiple felonies involving the use of a firearm. Specifically, on December 21, 1998, he entered guilty pleas for felony robbery, felony carjacking, and two counts of use of a firearm in the commission of a felony, all in Hampton County, Virginia. On February 8, 1999, he was found guilty at trial of felony use of a firearm and felony carjacking in Norfolk County, Virginia. CROCKETT received suspended and non-suspended incarceration sentences, as well as probation sentences, for these crimes. After having served much of a 20 year non-suspended incarceration sentence, he is currently serving his 25 year probation sentence. Upon his release from prison in Virginia, on June 26, 2016, his probation case was transferred to Wisconsin. He remains on probation until 2041.

7. CROCKETT has the following probation limitations prohibiting him from possessing, utilizing, or coming into contact with firearms or similar/related items: "Not possess or have within your access any firearm, ammunition, bullet proof vest or any object that resemble a firearm including but not limited to, BB guns, Pellet guns, Airsoft guns, Cap guns, starter pistols, holsters and magazine/clips. You shall not be in the presence of any person who is

in possession of a firearm (Legal or illegal) including being in a residence or vehicle where firearm is located. You shall not be on the premises of any gun or ammunition stores.”

8. On March 6, 2019, I received information from the Wisconsin Firearms Training Center (WFTC) at 12730 W. Burleigh Road in Brookfield, Wisconsin, that on November 3, 2017 CROCKETT purchased one AK-47, 7.62x39 30-round firearm magazine, four boxes of Winchester 12 gauge shotgun ammunition, one box of Sig ELT .380 Automatic Colt Pistol (ACP) ammunition, and one box of Federal American Eagle 7.62X39 rifle ammunition. He paid cash. As is standard procedure at WFTC, personal identifying information from CROCKETT’s identification card – *i.e.*, his driver’s license – was entered into their system. Specifically, the information in the WFTC transaction system identified the purchaser as: Roy L. CROCKETT, date of birth 02/26/1976, Wisconsin driver’s license number C623-7327-6066-00 expiring 02/26/2019, male, Brown eyes. That information matches CROCKETT’s precisely.

9. I know from my training and experience that an AK-47, 7.62x39 30-round firearm magazine can only be used with a semi-automatic or automatic AK-47, or variants of such rifles. I also know that Winchester 12 gauge ammunition is used with 12 gauge semi-automatic or pump action shotguns. Typically, this ammunition is used as a home-defense ammunition, not a hunting ammunition. I know that Sig ELT .380 ACP ammunition is used with .380 handguns or rifles. Finally, I know that Federal American Eagle 7.62x39 ammunition is used in weapons shooting the 7.62x39 caliber round. This ammunition can be used in the aforementioned AK-47 magazine and AK-47 rifle.

10. Based on my training and experience, I know that someone who purchases firearms magazines and ammunition necessarily has possession, custody, and control over that magazine and ammunition upon its purchase. That possession constitutes a violation by CROCKETT of 18 U.S.C. § 922(g).

11. Further, based on my training and experience, I know that someone who purchases firearms magazines and ammunition is likely purchasing those items for use with actual firearms. Therefore, there is probable cause to believe that CROCKETT made these purchases because he owns or has access to firearms. Given that he purchased three types of ammunition, it is reasonable to believe CROCKETT owns or has access to multiple types of firearms.

12. Firearms are durable goods. Unlike drugs, for example, which are often consumed or disposed of soon after their acquisition, individuals who possess firearms typically keep them for years. It is, therefore, reasonable to believe that CROCKETT still possess the firearms for which he was purchasing a magazine and ammunition in November 2017. It is also reasonable to believe Crockett still possesses the magazine, which is itself a durable good.

13. In addition to the purchase of the firearm magazine and the three types of ammunition, I have viewed a video of CROCKETT teaching an armed self-defense class involving the use of dry fire. Based on my training and experience, individuals utilize dry fire training to simulate the use of firearms in order to be prepared to use a firearm. On March 31, 2019, YouTube user Sy'Eir Williams posted a video entitled "OPERATION BLACK TACTICAL." The description reads: "Operation Black Tactical is a dry fire firearm simulated

training class aimed at teaching people the basics of armed self-defense and CQB.” I know from my training and experience that CQB is an abbreviation for Close Quarters Battle.

14. I viewed the referenced video, “OPERATION BLACK TACTICAL,” and visually identified CROCKETT in the video wearing a black hooded sweatshirt with the words “CAT” in yellow lettering, a yellow shirt under the sweatshirt, black sweatpants, and black baseball hat on backwards. In the video, CROCKETT is seen holding and manipulating a blue firearm, demonstrating firearms handling techniques. At one point in the video, CROCKETT is seen pointing the blue firearm at another person. CROCKETT is also seen pointing a firearm at a video screen depicting targets and pulling the trigger of the gun. Based on my training and experience as a State of Wisconsin Certified firearms instructor, I have used and trained with similar video systems. These systems are used to simulate the use of firearms training without the need for live fire ammunition and to simulate real life situations without the inherent dangers associated with the use of live fire ammunition. Though the firearms used in these systems vary by manufacture, they are designed to simulate the use of a real firearm and record where hits on the screen would be using a laser as if one were shooting with live ammunition.

15. On March 31, 2019 at 12:14pm, Facebook account “Sy’Eir Williams” (UID syeir.williams) posted a link to the YouTube video “OPERATION BLACK TACTICAL” referenced above. The Facebook account known to be utilized by CROCKETT (UID 100012708545338) was tagged in the post. I have visually identified that account as being utilized by CROCKETT based on his photographs and profile information. The post contained

the following: "Contact Roy Crockett to sign up for the next class." CROCKETT's Facebook account (UID 100012708545338) was tagged in the description.

16. A review of the "Roy CROCKETT" Facebook account with UID 100012708545338 revealed the account "liked" two pages related to firearms: "Jim Scoutten's Shooting USA" and "Trigger Happy Firearm Instruction LLC."

17. With regard to CROCKETT's residence, CROCKETT has been deceiving his Probation Officer about where he resides. Law enforcement interviewed CROCKETT's Probation Officer on 03/06/2019, who stated that CROCKETT has provided his residential address as 1826 N. 26th Street, Milwaukee, Wisconsin. CROCKETT reports that he lives at this residence with his mother. Furthermore, CROCKETT was issued a Wisconsin driver's license on 12/06/2016, at which time he provided the address of 1826 N. 26th Street, Milwaukee, Wisconsin. CROCKETT renewed the license on March 23, 2019 and again provided this N. 26th Street address as his residence.

18. Surveillance of CROCKETT has been conducted by FBI Milwaukee agents and task force officers on multiple occasions. During the time period between October 2018 and April 2019, including on April 5, 2019, CROCKETT has been observed to be residing at 7228 W. Sheridan Avenue, Milwaukee, Wisconsin. On October 1, 2018, CROCKETT made multiple trips with various household items, furniture, and boxes from 5003 N. 53rd Street, Milwaukee, Wisconsin, to the Sheridan Avenue residence. On each trip, CROCKETT used a key to unlock and lock the front door of the Sheridan Avenue residence. Thus, there is probable cause to

believe CROCKETT currently resides at 7228 W. Sheridan Avenue, Milwaukee, Wisconsin, the SUBJECT PREMISES.

19. On numerous occasions during surveillance conducted between June 2018 and April 2019, including on 04/05/2019, CROCKETT was observed while driving VEHICLE 1, a 1997 black Ford F-150 pickup truck bearing Wisconsin license plate ND2966. This vehicle is registered to Roy Lee CROCKETT, date of birth 02/26/1976. VEHICLE 1 has also been observed on multiple occasions during surveillance parked in the driveway and in front of the SUBJECT PREMISES.

20. VEHICLE 2, a gray 2001 Mercedes Benz ML bearing Wisconsin license plate ACR9300, has also been observed on numerous occasions to be parked in the driveway at the SUBJECT PREMISES. On 04/05/2019, during a surveillance operation targeting CROCKETT, CROCKETT was observed exiting the SUBJECT PREMISES, opening a rear door and then the rear hatch of VEHICLE 2 while it was parked in the driveway, retrieving a white bag containing unknown items from inside the vehicle, and then returning with said bag back into the SUBJECT PREMISES.

21. Based on my training and experience, individuals who possess firearms store them (and associated magazines and ammunition) in their residences. And in my training and experience, individuals who possess firearms also store and transport firearms and ammunition in their vehicles. The fact that CROCKETT teaches firearms training courses to which he must drive makes it particularly likely he stores and transports firearms in his vehicles.

22. Based on my training and experience, individuals who possess firearms also use computers with access to the internet to research, buy, and sell firearms and ammunition. Based on my training and experience websites are available to allow seller to buyer purchases of firearms without federal background checks. Such individuals also often store photographs of themselves in possession of firearms and ammunition on their computers, including their camera- and internet-enabled mobile phones, and share such photographs via the internet. It is reasonable to believe that if CROCKETT has a computer in his residence that it will contain evidence of violations of 18 U.S.C. § 922(g).

23. On April 26, 2019, CROCKETT was arrested at his work place, the Milwaukee Housing Authority. He had firearm magazines and ammunition on his person at the time of his arrest.

24. In the automobile CROCKETT drove to work, VEHICLE 1, a 9mm M&P handgun was stored in the space between the driver's seat and the center console.

25. Law enforcement saw CROCKETT bring a black backpack with him when he drove to his workplace, the Milwaukee Housing Authority. After CROCKETT'S arrest, the Milwaukee Housing Authority allowed FBI TFO Brett Huston to take custody of the black backpack (which had been left on the Milwaukee Housing Authority premises). The backpack was secured to avoid the destruction of any potential evidence, but it was not opened. In light of the magazines and ammunition found on CROCKETT'S person at the time of the arrest, and in light of the handgun found in VEHICLE 1, there is probable cause to believe evidence of a violation of Section 922(g) will be found in CROCKETT'S backpack.

26. CROCKETT also had in his possession a Motorola Model XT1924-7 mobile phone with IMEI 354138095267589. In my training and experience, individuals often take photographs of themselves with their firearms and those photographs are stored on their mobile phones. Individuals who possess firearms and ammunition also often use their mobile phones to research and purchase firearms and ammunition. Thus, there is probable cause to believe evidence of a violation of Section 922(g) will be found in CROCKETT'S mobile phone

27. Upon a search of Crockett's home, 7228 W. Sheridan Avenue, Milwaukee, Wisconsin, law enforcement found multiple pieces of mail addressed to CROCKETT (though at the address "1826 N. 26th Street. Milwaukee, Wisconsin").

28. Law enforcement also found in the SUBJECT PREMESIS, *inter alia*, two 12-guage loaded shotguns, at least six-hundred rounds of ammunition, one bulletproof vest, two sets of handcuffs, two stun guns, four training pistols, four rifle magazines, and multiple handgun and rifle accessories.

III. TECHNICAL TERMS

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

- b. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IV. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

30. As described above and in Search Warrant Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PHONE, in whatever form they are found. One form in which the records might be found is data stored on a phone's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. I submit that there is probable cause to believe records will be stored on the SUBJECT PHONE's storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file

on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

32. *Forensic evidence.* As further described in Search Warrant Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes

how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PHONE because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information

stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created.

The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

33. *Nature of examination.* Based on the foregoing, and consistent with Federal Rule of Criminal Procedure 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

V. CONCLUSION

34. Based on my training and experience and the facts set forth in this affidavit, I submit that there is probable cause to believe evidence of violations of 18 U.S.C. § 922(g) will be found on CROCKETT's mobile phone and in the backpack recovered at the time of CROCKETT'S arrest for violating 18 U.S.C. § 922(g) .

ATTACHMENT A

Property to be searched

The property to be searched is more particularly described as:

Motorola Model XT1924-7 mobile phone with IMEI 354138095267589; and

Black nylon Eastsport backpack.

ATTACHMENT B

Property to be seized

1. All firearms, firearm parts (including but not limited to magazines), firearm accessories, firearm packaging, and ammunition;
2. All records on the device described in Attachment A that relate to violations of 18 U.S.C 922(g), those violations involving Roy Lee Crockett, Jr. and occurring after June 26, 2016, including:
 - a. Any identifying information;
 - b. Photographs, videos, or other media storage connected to firearms;
 - c. Types, amounts, and prices of firearms purchased/sold;
 - d. Any information related to sources or purchasers of firearms (including names, addresses, phone numbers, or any other identifying information);
 - e. All bank records, checks, credit card bills, account information, and other financial records related to firearms commerce.
 - f. Evidence of user attribution showing who used or owned the DEVICES A-I at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
 - g. Records evidencing the use of the Internet Protocol address, including:
 - i. records of Internet Protocol addresses used;

- ii. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

4. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;

- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.